CSCI 1800 Cybersecurity and International Relations

Economics of Cybersecurity

John E. Savage
Brown University
What is Cyber Economics?

• Study of economics of computer & network security
• Some roles for economics in security:
  – Insurance can indemnify policyholders against loss due to interruption of service, fraud, etc.
  – Insurance premiums can be reduced in return for reporting cyber incident data. Will also allow insurance companies to better price their products.
  – Requiring companies to assume liability for the quality of their products should incentivize them to produce better, more secure products.
  – Insurance companies can offer advice to reduce the threat of cyber losses
Outline

• Since many cybersecurity problems are economic, modest incentives can significantly improve security.

• Four areas are examined
  – Online identity theft, industrial espionage, critical infrastructure protection, and botnets.

• Three economic challenges:
  – Misaligned incentives, information asymmetries, and externalities.

Some Cybersecurity Applications

• Online identity theft
  – Primary way cybercriminals steal from individuals.

• Industrial cyber espionage
  – Trade secrets remotely stolen; theft not detected.

• Critical infrastructure protection
  – Industrial control systems vulnerable & not protected

• Botnets
  – Common and involved in many types of attack.
Online Theft

• E-banking makes it much easier to steal identities
  – Security and authentication have not kept pace.
  – Malware can install key loggers.

• 2013 report by Center for Strategic and International Studies and McAfee estimates annual loss of $100 Billion to US economy and 508,000 jobs
Industrial Cyber Espionage

• Operation Aurora launched in 2009.
  – Google revealed attack and eventually stopped offering its search service inside mainland China.
  – The attack targeted *repositories* of Google and more than 30 other companies.
  – It received a great deal of press and government attention.

• Were files just stolen or were they modified?

• Mandiant 2013 APT1 report shows this was tip of the iceberg. [http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)
Critical Infrastructure Protection

• Example:
  – Idaho National Lab experiment (also called Aurora) that destroyed an power generator. See http://www.youtube.com/embed/rTkXgqK1I9A


• SCADA¹ systems are involved in almost all sectors. They are considered poorly protected.

1. SCADA: Supervisory Control and Data Acquisition
Economic Barriers to Cybersecurity

• Misaligned incentives
  – E.g. If those responsible for protecting a system don’t pay for security violations, no incentive to keep it safe.

• Information asymmetries
  – Absence of critical information can lead to poor decisions that alter markets.

• Externalities
  – Costs incurred by others not party to transactions.
  – E.g. air pollution reduces a manufacturer’s cost but increases cost to society.
Misaligned Incentives

• If those acquiring systems, don’t pay a price for failure to meet specs, failures are more likely.
  – E.g. Consider purchase of a medical records system
  – E.g. Electricity companies save money by replacing atomic clocks with GPS. When a solar flare wipes out GPS, the public pays the price.
Misaligned Incentives

• There is a natural tension between efficiency and resiliency in design of IT systems.
  – Critical infrastructures used to be operated on separate networks. E.g. ATT network (SS7), SCADA systems
  – Efficiency drives us toward network convergence. We are now heavily dependent on Internet.
  – Who is concerned about the unintended consequences?
    • 3/2/14 NYT article “Power Grid Preparedness Falls Short ...”*

• Efficiency often trumps security.
• When security fails, cost often borne by the public.

Information Asymmetries

• Incident data is essential but hard to obtain.
  – Unless can’t be ignored, e.g. Target, Home Depot attacks
  – Reputations (stock prices) are on the line.
  – Companies don’t want to reveal vulnerabilities.

• Asymmetric information can be deleterious:
  – Ackerlof (2007 Nobel) explained pricing of auto “lemons”
  – If market has 50 “good” used cars @ $2K and 50 lemons @ $1K but customers can’t tell them apart, price drops well below $2K. Owners of good cars will not sell. Market gets filled with lemons.
  – Buyers won’t pay premium for quality that can’t be measured
Externalities

• Network externality:
  – The tendency of large firms to dominate markets results from benefits of interoperability.
    • Think Facebook, Windows, etc.
  – Individuals lose control over issues such as privacy.

• Poor security creates negative externality:
  – Underinvestment in security may impose burden on others. E.g. botnets, insecure power grid, national security.
Externalities

• Independent security:
  – Free riding: If investment in security by others protects you, why would you invest in your own protection?
Is Regulation the Solution?

• Topics we examine:
  – Ex Ante Safety Regulation vs Ex Post Liability
  – Information Disclosure
  – Cyber-Insurance
  – Indirect Intermediary Liability
Ex Ante Safety Regulation vs Ex Post Liability

• Ex ante goal: prevent accidents in advance.
  – 1999 Gramm-Leach-Bliley Act – repealed Glass-Steagall Act of 1933 & allowed affiliations between commercial banks and securities firms. (See Crash of 2008!)

• Ex post liability – threat of monetary damages
  – Would this push Microsoft to make code more secure?
    • They are making progress without it. Or are they aware of cost?
  – Ex post liability has a negative externality – it would reduce pace of innovation.
  – Without changes in coding techniques, software security may not increase.
Ex Ante Safety Regulation vs Ex Post Liability

• Unfortunately, security errors are unavoidable.
• Would results be better if vendors were held to a higher standard of coding and testing?
• In some sectors, best to use both approaches.
  – However, ex ante regulation doesn’t work well when regulator lacks information about harms or is uncertain about minimum standards.
  – Also, ex post liability doesn’t work when firms not always held responsible or they can’t pay.
• These conditions often hold in cybersecurity.
Information Disclosure

• Since information asymmetries are barrier to cybersecurity, info disclosure may be the answer.
  – “Sunlight is the best disinfectant” – Justice Brandeis
  – Community has a right to know.

• Law requires disclosure of toxic chemicals released into the environment.
  – This law has reduced the amount of such chemicals.
  – The Whitehouse-Kyl Cyber Security Public Awareness Act of 2011 might have done the same for cyber.

See http://www.gpo.gov/fdsys/pkg/BILLS-112s813is/pdf/BILLS-112s813is.pdf
Information Disclosure

• Target 2013 breach estimated to cost $252 Million!
• In 2015, 47 states had privacy breach notification laws
  – They require private or government entities to notify individuals of breaches of personally identifiable info.
  – Companies are now much more aware of risks
  – It appears that the laws have reduced fraud
• Failure to publicize breaches exposes to similar risks those not informed.
• Information sharing and analysis centers (ISACs) are closed industry groups set up by DHS to protect the critical infrastructure. Effective! They don’t publicize data.
Cyber-Insurance

• Coverage provided for data breaches, business interruption, and network damage.
• Offers incentives to take precautions
• Rewards investment by lowering premiums
• Encourages data collection, dealing with informational asymmetries.
• Smooths out financial outcomes – small fixed present cost offsets future large losses.
Cyber-Insurance

- Cyber-insurance market small for long time despite optimistic projections of its growth.
- Premiums based on company size, not observed security levels.
- What is wrong with cyber-insurance industry?
  - On supply side: Hard to measure security levels
- Interest in cyber-insurance is growing*

* See http://blogs.wsj.com/cio/2015/04/13/companies-seeking-common-ground-on-cybersecurity-turn-to-insurers/
Indirect Intermediary Liability

• Liability doesn’t have to be placed on the party directly responsible for harm.

• Usually 3 players: bad actor, victim, third party.
  – E.g. Employers responsible for actions of employees

• It works when
  – Bad actor inaccessible, can’t be identified, or can’t pay if caught.
  – Too costly to design contracts that assign blame fairly.
  – Third party can detect or prevent harm and can internalize negative externalities by reducing # bad acts.
Indirect Intermediary Liability

• Lichtman and Posner (2004) argue that these conditions apply to ISPs as third parties.
  – For what types of behavior could ISPs play this role?

• ISPs exempted from liability for defamatory content of subscribers (1996 Communications Decency Act)
  – Gave license to ISPs to monitor posts by users.

• DMCA exempts ISPs from copyright violations if they comply with “notice-and-takedown” requests.

• To stop online gambling, credit card cos. made 3rd parties
Indirect Intermediary Liability

- The FCC announced in 2012* that ISPs representing more than 90% of US Internet users have agreed to take voluntary action against the following cyber threats:
  - Anti-bot Code of Conduct
  - DNS Best Practices
  - IP Route Hijacking Industry Framework

Indirect Intermediary Liability

• Credit card fraud makes bank the intermediary when fraud occurs at brick and mortar establishments but makes the merchant the intermediary for online transactions.
  – The reason apparently is that online transactions are considered more risky.
  – This treatment of fraud could change over time
Recommendation #1: Infected Bots

- Tyler Moore’s program for malware remediation
  - ISPs obliged to act on notification of customer infection by helping to clean up customer computer. In return, ISPs exempted from liability. Else, liable.
  - Cost of cleanup shared by ISPs, government, software vendors and consumers.
  - Reports of infection sent to public DB (report ISP, OS type, infection vector, time to remediation, and fix.)
  - Software vendors pay for cleanup in proportion to number of reported infections of their software.
  - Consumer contribution capped. They cannot be disconnected if they cooperate in cleanup.
Cleaning Up Infected Bots

• Comcast ran trial program to notify customers of infection. They offered service together with McAfee anti-virus (AV) to clean up machines.
• ISPs can quarantine machines and then require AV and malware removal tools be downloaded.
• Quarantine puts burden on user and cost on ISP
Cleaning Up Infected Bots

• Situation unsatisfactory. What should be done?
  – Can encourage ISPs to help customers – very weak.
  – Can use DMCA as model. Give immunity to ISP if they help cleanup infected computers. Make them responsible if they don’t.

• Must have
  – Fair distribution of cost of cleanup
  – Transparency via mandatory disclosure of infections
  – Protection of consumer connections.
Recommendation #2: Disclosure

- Regularly publish aggregated losses due to online banking and payment cards.
  - Incident figures
  - Victim bank demographics
  - Victim demographics
  - Attack vectors
  - Business category
- Such info can help decide security measures.
Disclosure

- FBI runs Internet Crime Complaint Center (IC3)
- Financial services ISAC data kept in closed circle.
  - Because ISACs have voluntary disclosure systems, financial services industry does not internalize the cost of insecurity.
- Users also need to know where fraud occurs.
- Disclosure would help decide if more secure credit card technologies should be used.
Recommendation #3: SCADA Incidents

• Make disclosure of control system incidents and intrusions mandatory to the relevant ISACs who then publicly disseminate them.

• Anonymous intelligence officials say that Chinese and Russians are regularly intruding into US electrical grid. However, grid VPs have no knowledge of this!
Recommendation #4: Espionage

• Aggregate and report cyber espionage and report to WTO.

• Industrial espionage is a significant problem for American companies.

• They don’t report intrusions for fear of damaging their reputations.
  
  – Did the Google Aurora caper signal a change?
Conclusion

• Economic perspective essential to understand cybersecurity today and improve it.

• Principal recommendations:
  – Get ISP to take more active role in ridding malware
  – Collect and publish data on a range of security incidents.
  – Raise awareness of the issues and assign responsibility for action.